OS2faktor Login

Implementeringsplan

Version: 1.2.0
Date: 23.03.2022
Author: BSG

Indhold

1 Indledning

Dette dokument er et udkast til en implementeringsplan for OS2faktor Login, og kan anvendes som et udgangspunkt til at danne en fuld implementeringsplan i en given kommune.

Formålet med dokumentet er at synliggøre de aktiviteter der som minimum skal udføres for at være klar til at anmelde løsningen til Digitaliseringsstyrelsen, så den kan anvendes til som Lokal Identity Provider overfor NemLog-in 3.

2 Samlet overblik over aktiviteter

Nedendestående overblik kan ses som en liste over aktiviteter der er nødvendige for en fuld implementering af OS2faktor Login. Listen indeholder aktiviteter som ligger udenfor Løsningen, men som er nødvendige for at blive endeligt revideret og anmeldt til Digitaliseringsstyrelsen.

Nogle af punkterne i denne liste er yderligere udpenslet i de efterfølgende afsnit, og beriget med andre aktiviteter som kan være relevante at udføre også (men som ikke er krævede)

- Teknisk installation af OS2faktor Login
  - Indlæsning af stamdata
  - Integration til AD til password reset
  - Lav pakker/images til udruldning af Windows Credentials Provider
  - Lav pakker/images til udruldning af 2-faktor klienter til slutbrugerne
  - Indgå serviceaftaler og opsætning til CPR og Digital Post på Serviceplatformen
  - Integration til NemLog-in3 (tjenesteudbyder)
- Pilotafprøvning af den tekniske installation
  - Vælg én eller flere fagsystemer hvor Login løsningen skal anvendes mod, og opsæt formål og tidsplan for afprøvningen (fx afprøvning af vejledninger, 2-faktor klienter osv)
  - Lav en afprøvning af password reset
  - Lav en afprøvning af 2-faktor klienterne og vælg hvilke der ønskes anvendt
- Opsætning/konfiguration
  - Tilpas password politikker
  - Tilpas anvendelsesvilkår
  - Tilpas lede- og hjælptekster
  - Tilpas privatlivspolitik
  - Vælg og opsæt administratorer i OS2faktor Login, herunder oplæring af administratorerne i anvendelsen af OS2faktor Logins administrative portal
- Implementer ISO 27001
  - Udarbejde en Statement of Applicability (SOA)
  - Udarbejde alle nødvendige procedurer
  - Implementere procedurerne i et eller flere årshjul
  - Sikre at alle procedure er blevet udført mindst én gang, og at der er opsamlet dokumentationsspor på at procedurerne er gennemført
- Besvar NSIS kravene i Bilag A
  - Gennemgå alle kravene, og fordel ansvaret for besvarelsen til relevante aktører
  - Gennemgå alle besvarelser og sikre at de hænger sammen og send til revisoren til check-up (eller hvad der nu er aftalt med revisoren)
- Organisatorisk implementering
  - Fuld udruldning af 2-faktor klienter og windows credentials provider til slutbrugerne
  - Sikre at alle medarbejdere har fået aktiveret deres erhvervsidentitet

- Få udført revision og anmeld løsningen til Digitaliseringsstyrelsen

3 Tekniske forudsætninger

I forbindelse med implementeringen af OS2faktor Login er der en række data-adgange der skal etableres. Disse er beskrevet i dette afsnit, og går på tværs af alle typer af anvendelser

3.1 Integration til CPR opslag på Serviceplatformen

OS2faktor Login har brug for at ajourføre navne på registrerede brugere, så disse afspejler deres faktiske folkeregisternavn. Til dette formål anvendes et CPR opslag på Serviceplatformen.

Digital Identity anmoder om en Serviceaftale, som skal godkendes af Kommunen.

3.2 Integration til Digital Post via Serviceplatformen

OS2faktor Login kan anvendes til at sende beskeder til brugernes e-boks med engangs-pinkoder til aktivering og/eller kodeordskifte. Denne funktionalitet anvendes kun hvis man ønsker at medarbejdere kan fravælge digital identitetssikring vha NemID eller MitID.

Hvis man gør brug af den såkaldte "Registrant" funktion i OS2faktor Login, er det nødvendigt at opsætte en integration til Print snitfladen på Serviceplatformen. Denne snitflade kan sende beskeder med aktiveringskoder til disse brugeres e-boks, som så kan bruges til at gennemføre identitetssikringen i forbindelse med udstedelse og re-aktivering af deres erhvervsidentitet.

Digital Identity anmoder om en Serviceaftale, som skal godkendes af Kommunen.

Efterfølgende skal Kommunen opsætte en såkaldt "rute" på Serviceplatformen, der angiver hvordan beskeder fra OS2faktor Login skal routes til e-boks. Til det formål har KOMBIT udarbejdet en vejledning. De relevante afsnit er Bilag D (vejledningen) og Bilag A (blanketten som skal udfyldes).

https://digitaliseringskataloget.dk/integration/sf1600

https://docs.kombit.dk/integration/sf1600/2.5/pakke

Det sidste link er til en ZIP fil, der indeholder endnu en ZIP fil (SF1600 Bilag 20200716.zip). I denne sidste ZIP fil ligger "Vejledning til Print 2.1.pdf", som har hhv Bilag A og Bilag D som skal bruges til denne rute-opsætning.

3.3 Integration til NemLog-in3 (MitID privat) som identifikationsmekanisme

OS2faktor Login skal foretage en identitetssikring af brugeren i forbindelse med udstedelsen (og reaktivering) af erhvervsidentiteter. Til formålet anvendes pt NemID og på sigt MitID.

Muligheden for at anvende MitID Privat som elektronisk identifikationsmiddel bliver muligt efter sommer 2022, hvor OS2faktor Login overgår til at anvende NemLog-in3 som elektronisk identifikations-broker. NemLog-in3 vil sikre at både NemID og MitID kan anvendes som identifikationsmiddel.

Når dette er muligt, opdateres denne vejledning med de nødvendige skridt for at opsætte integrationen til NemLog-in3.

Indtil dette tidspunkt anvendes OS2faktor's eksisterende NemID integration til identitetssikring.

4 Opgaver og milepæle

I dette afsnit er der liste af opgaver der skal udføres i forbindelse med implementeringen, samt de milepæle man kan vælge at arbejde mod undervejs i implementeringen.

4.1 Opgaver

4.1.1 Databehandleraftale og driftsaftale

Der skal indgås en databehandleraftale og driftsaftale inden løsningen tages i brug. Dette bør igangsættes som noget af det første, da overførsel af data til løsningen forudsætter en Databehandleraftale.

4.1.2 Vælge hvilke bruger-domæner der er i scope

Løsningen kan anvendes på mange forskellige bruger-domæner, fx

- Brugere i det administrative domæne (typisk kommunens administrative AD)
- Ansatte på instititionsområdet (Dagtilbud, Skole/SFO), typisk hentet fra kommunens skole AD
- Elever på skole-området
- Eksterne (fx konsulenter, revisorerer, samarbejdspartnere, osv)

Man kan implementere de enkelte bruger-domæner uafhængigt af hinanden, men man bør lægge en plan for hvilken, eller hvilke, bruger-domæner man vil implementere først.

4.1.3 Teknisk implementering "per domæne"

For hvert bruger-domæne skal der udføres en teknisk og organisatorisk implementering, som beskrevet nedenfor.

Valg af datakilde til bruger-domænet

OS2faktor Login forudsætter at kommunen leverer lister over de personer som må anvende løsningen, herunder hvilke af disse personer som må få en såkaldt erhvervsidentitet.

Kommunen kan via disse lister styre både oprettelse og nedlæggelse af erhvervsidentiteter, og da disse processer er under revision, er valget af kilde noget der påvirker de revisionspligtige arbejdsprocesser.

Man kan fx vælge at basere udtrækket på Active Directory, og styre hvem der må få en erhvervsidentitet ud fra et bestemt gruppemedlemsskab. Her vil de revisionspligtige processer dække udtrækket fra AD, og styringen af gruppemedlemskabet.

Man kan ligeledes vælge at kilden skal trækkes fra en lokal organisationsløsning som SOFD Core, OS2mo, APOS eller måske et lokalt IdM system. Dette vil på lignende måde påvirke hvilke processer der vil være under revision.

Man bør som minimum afdække

- Hvem har adgang til at redigere den kilde data trækkes fra
- Hvem har adgang til den software der foretager udtrækket af data og overførslen til OS2faktor Login

- Hvilke processer vil det være nødvendigt at dokumentere, for at kunne gennemføre en revision af dette område

Følgende data skal kunne leveres fra datakilden til OS2faktor Login

- CPR nummeret på personen
- Navnet på personen (anvendes kun initielt, og vil blive opdateret fra CPR registeret efterfølgende)
- Angivelse af om personen må få en erhvervsidentitet (ja/nej flag)

Det er også muligt at angive følgende ekstra oplysninger fra kilden, som dog ikke er krævede

- E-mail adressen på personen
- AD Brugerkontonavn (nødvendig hvis der ønskes password replikering til AD)

Teknisk integration til datakilden

Når kilden til bruger-domænet er valgt, skal der opsættes en teknisk integration der kan udlæse data regelmæssigt. OS2faktor Login har integrationer til

- Active Directory
- Azure AD
- SOFD Core

Som fungerer "ud af boksen". Man kan også vælge at få Digital Identity til at udføre en integration til en anden kilde, eller man kan udvikle en selv (evt i samarbejde med en anden leverandør). Der findes REST snitflader til selve indlæsningen af kildedata.

Hvis man vælger en af standard-integrationer, så kan dette sættes op på 1-2 timer sammen med kommunens it-teknikere.

Password replikering / Password reset

OS2faktor understøtter replikering af kodeord til Active Directory og Azure AD. Det anbefales at man får sat denne integration op, da den også fungerer som en generel Password Reset løsning.

Opsætningen foretages i samarbejde med kommunens teknikere, og tager 1-2 timer at udføre.

4.1.4 Pilot-afprøvning "per domæne"

Det anbefales at man udfører en pilot-afprøvning, hvor man anvender OS2faktor Login som login-løsning til en eller to afgrænsede it-systemer, evt i samspil med en udvalgt gruppe af pilotbrugere.

Formålet er at indsamle viden omkring anvendelsen af løsningen, så både kommunens it-afdeling og servicedesk er bekendt med løsningen inden den implementerings bredt i kommunen-

Den viden der indsamles kan samtidig anvendes til at udarbejde den relevante information til resten af medarbejderene, så de kan klædes på inden ibrugtagningen af løsningen.

Man bør afsætte 2-3 kalenderuger til pilotafprøvning.

Den tekniske opsætning af integrationen til de udvalgte it-systemer foretages af Digital Identity, evt i samspil med kommunens it-afdeling, og vil typisk tage 1-2 timer.

4.1.5 Organisatorisk implementering "per domæne"

Efter afsluttet pilot-afprøvning, bør man afsætte 1-2 kalenderuger til at klaregøre den information som slutbrugerne skal have.

Herefter er man klar til at starte den organisatoriske implementering, og man bør udvælge 1-2 større it-systemer og/eller infrastrukturer hvor OS2faktor Login løsningen skal anvendes som generel login løsning.

Dette kunne være

- KOMBITs Context Handler
- STIL UniLogin Broker
- Arbejdsmarkedsløsningen
- AULA
- EOJ
- ... andre fagsystemer

Medarbejderne skal informeres om den kommende ændring til login løsningen, og evt udstyres med en OS2faktor MFA klient hvis fagsystemet forudsætter 2-faktor login.

Der findes en række OS2faktor MFA klienter, hvor flere af dem kan rulles ud systematisk, så de automatisk dukker op på brugernes smartphones og/eller PC'ere. Denne udruldning bør planlægges med kommunens it-afdeling, og man bør afsætte 1-2 kalenderuger til teknisk afprøvning af udruldningen og MFA klienterne, hvis man ikke allerede anvender OS2faktor MFA klienterne i sin kommune.

4.1.6 Implementation af erhvervsidentiter

Den sidste implementeringsopgave vedrører erhvervsidentiteterne. Der er ingen tekniske krav om brugen af erhvervsidentiteter, og kan man vælge at angive at ingen medarbejdere skal have en erhvervsidentitet i den initielle implementering, for ikke at forstyre medarbejderne med den del.

Når en medarbejder kan få en erhvervsidentitet (angivet via indlæsning af data fra kilden), så vil medarbejderen blive tilbudt aktivering af deres erhvervsidentitet når de anvender løsningen.

Denne aktivering vil typisk blive udført ved anvendelse af brugerens NemID. Denne aktivering skal kun ske en enkelt gang, hvorefter erhvervsidentiteten er udstedt, og brugeren kan nu foretage logins til fagsystemer og/eller infrastrukturerer der stiller krav om en erhvervsidentitet (dvs et login der overholder NSIS kravene).

Hvis en bruger ikke ønsker at anvende sin erhvervsidentitet, skal der foretages en manuel aktivering af medarbejderen via fremmøde hos borgerservice/servicedesk i kommunen.

Man bør derfor klæde de ansvarlige medarbejdere på (typisk vil man vælge borgerservice til at håndtere denne arbejdsopgave, men det kunne også være kommunens servicedesk), så de ved hvordan de skal foretage denne manuelle registrering.

Følgende opgaver bør udføres i forbindelse med denne opgave

- Udarbejde information til alle medarbejdere om den registreringsproces der skal gennemføre ved aktivering af deres erhvervsidentitet

- Udarbejde vejledninger til Borgerservice/Servidesk, så de ved hvor og hvordan de kan udføre den manuelle aktivering af medarbejdere der ikke ønsker at anvende deres NemID

4.1.7 Revision

Man kan godt begynde udstedelsen af erhvervsidentiteter inden løsningen er revideret, men man kan ikke anvende disse erhvervsidentiteter før løsnignen er revideret og anmeldt til Digitaliseringsstyrelsen.

Revisionen kan udføres når følgende opgaver er på plads

- Man har modtaget en revisionsrapport fra Digital Identity for OS2faktor Login løsningen
- Bilag A i revisionsanmeldelsen er udfyldt (med henvisninger til den revisionsrapport man har modtaget fra Digital Identity i alle de punkter hvor det er muligt)
- Alle punkter i Bilag A er implementeret i kommunen som beskrevet

Det konkrekte revisionsforløb bør man aftale med sin revisor.

Når revisionen er udført, skal man anmelde sin løsning til Digitaliseringsstyrelsen. Det sidste er en forudsætning for at kunne udføre den tekniske integration til NemLog-in3 i næste punkt.

4.2 Teknisk integration til NemLog-in3, m.m.

Digital Identity sørger for at løsningen bliver integreret til NemLog-in 3, og andre NSIS infrastrukturer som kommunen ønsker at anvende løsningen mod (fx STILs UniLogin broker).

Typisk vil det kræve at kommunen godkender opsætningen, hvilket gøres via hvad end administrativ portal som integrationsparten tilbyder (fx NemLog-in3 administrationsportalen).

4.3 Milepæle

Undervejs i implementeringen kan man høste nogle gevinster. Man kan tage disse i brug uden at være helt færdig med implementeringen. Disse er

- Password Reset funktionalitet
- Ny (forbedret) login løsning til erstatning af eksisterende AD FS integrationer
- NSIS anmeldelse og erhvervsidentiteter

5 Udfasning af gamle løsninger

OS2faktor Login vil kunne erstatte en række eksisterende løsninger i kommunen, og man bør være bevidst om hvilke disse er, så man kan udfase dem, og evt spare licenser, efterhånden som OS2faktor implementeringen gør det muligt.

Typiske systemer som kan udfases er

5.1 Andre Identity Provider løsninger

Hvis man har andre Identity Provider løsninger i kommunen, kan man udfase disse når man har flyttet alle integrationer fra disse løsninger over på OS2faktor Login.

Hvis man påtænker udfasning af sin eksisterende Identity Provider løsning, bør man prioritere at flytte integrationer på denne til OS2faktor Login, så man tidligt kan lukke den gamle løsning.

5.2 Andre MFA klienter

Hvis man gør brug af andre MFA klienter til 2-faktor login, kan man overveje om disse skal erstattes helt af den MFA klient der følger med OS2faktor Login løsningen.

En afdækning af hvilke MFA klienter man har i kommunen, og hvor de anvendes, kan være relevant input til en prioriteret udfasning af disse.

5.3 Signaturcentralen

Man bør afdække hvor man anvender den gamle medarbejdersignatur. Når man ikke længere anvender den gamle medarbejdersignatur nogen steder, kan man udfase Signaturcentralen.

Hvis man har enkelte systemer tilbage der stadig gør brug af Signaturcentralen, og det vurderes at tage langt tid før disse lukkes ned, så kan man evt overveje om Signaturcentralen giver nok værdi i forhold til om den skal udfases før tid. I så fald vil brugerne skulle anvende deres medarbejdersignatur som en klassisk nøglefil.

5.4 Andre Password Reset løsninger

Hvis kommunen anvender andre password reset løsninger, kan disse erstattes af OS2faktor Login når man har implementeret password replikeringen til AD fra OS2faktor Login.